Christyne M. Martens WSB #7-5044
Assistant United States Attorney
District of Wyoming
P.O. Box 22211
Casper, WY 82602
307-261-5434 (phone)
307-261-5471 (fax)
christyne.marents@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF WYOMING

UNITED STATES OF AMERICA, Plaintiff, **v.** **DAMIEN ELRIC HUGHES,** Defendant.	**Docket No. 23-CR-159-J**

GOVERNMENT'S NOTICE OF INTENT TO OFFER EXPERT TESTIMONY

The United States of America hereby submits its notice of intent to offer expert testimony. Fed. R. Crim. P. 16(a)(1)(G). The United States reserves the right to further supplement this notice.

SPECIAL AGENT GARY SEDER, WYOMING DIVISION OF CRIMINAL INVESTIGATION

Qualifications: Gary Seder is a Special Agent with the Wyoming Division of Criminal Investigation (DCI), stationed in the Cheyenne, Wyoming, field office and has been so employed since February 2022. SA Seder has over 30 years of law enforcement experience. Prior to his employment with Wyoming DCI, SA Seder was with the Montana Department of Justice, Division of Criminal Investigation, the Yellowstone County Sheriff's Office and Bighorn County Sheriff's Office. SA Seder has specialized training to target and identify persons such as those using the Internet to possess, produce and distribute child pornography. Specifically, SA Seder has over 12 years of experience in internet investigation techniques with a focus towards digital evidence,

wireless and other Internet access basics, and instruments of child exploitation. He has approximately 10 years of experience conducting investigations as part of the Internet Crimes Against Children taskforce, including four years as the Montana ICAC Commander.

To conduct these types of investigations, SA Seder has specialized training in online undercover techniques for chat investigations and peer to peer file sharing networks. SA Seder has numerous computer related certifications as well other certifications in the area of law enforcement. Additional qualifications, training and experience for SA Seder are further outlined in his Curriculum Vitae, which is attached as *Exhibit 1*.

SA Seder's duties and responsibilities as a DCI Special Agent are: conducting state and federal investigations related to technology-facilitated crimes; conducting certified computer forensic examinations on computers, computer equipment, digital media, digital cameras, cellular phones, and all peripherals involved in Internet Crimes Against Children and Narcotics Trafficking; serving arrest warrants, executing search warrants; and developing criminal cases for presentation before the courts in state and federal venues.

SA Seder has authored no publications within the past ten years and has not testified as an expert at trial or by deposition within the past four years. Fed. R. Crim. P. 16(a)(1)(G)(iii).

***Summary of Testimony**:* SA Seder would testify about his role in the investigation in this case and the opinions he has reached based on his investigation. SA Seder would further testify regarding how child exploitation investigations are conducted, including his knowledge of the use of abbreviations and acronyms used by individuals in these investigations. He would further testify regarding his investigation, preservation, and retrieval of digital information from the digital devices seized from the Defendant. SA Seder would testify regarding the procedures he used to

preserve and analyze the items seized from the Defendant's digital devices and would testify to the opinions and conclusions he reached based on his investigation. SA Seder would provide percipient and opinion testimony as to the forensic downloads and extraction of digital information from the digital devices seized during the investigation of this case. SA Seder would testify regarding the investigation, preservation, and retrieval of digital information from the digital devices. SA Seder would testify regarding the procedures used to preserve the data contained on the seized digital devices and the process of extraction of the data from the digital devices using specific software, and the analysis of the devices. SA Seder would testify as to what files were found on which of the Defendant's devices and how they were stored on said devices. Specifically, SA Seder would set forth the findings of the forensic examinations of the digital devices and the various files that were discovered during the examinations and will render an opinion consistent with reports and other information provided in discovery, including that the Defendant operated the devices and accounts at issue, that the Defendant used the devices and accounts in the charged conduct, and that the Defendant's accounts and devices were not hacked.

SA Seder would further testify how it is extremely common for child pornography users to have social media, email accounts, and cloud storage. SA Seder would explain to the jury how different social media platforms operate, and how individuals upload files, photos, and videos on servers, to a cloud storage which allows members to access them from any computer with an internet connection. SA Seder would further explain how individuals use social media, email, and cloud storage to share different types of media without physically storing information on their own personal electronic devices and how that information can be downloaded to a device. He will explain that using mobile devices to access messaging applications, social media, email accounts,

peer to peer file sharing, and cloud storage uses a combination of the internet and cellular telephone networks. He will explain that using computers to access messaging applications, social media, email accounts, peer to peer file sharing, and cloud storage uses the internet.

SA Seder will explain that it is common for child pornography distributors and possessors to store contraband on personal digital devices and make illicit content available to other internet users through various file-sharing interfaces. He will explain that it is also common for child pornography distributors and possessors to store child erotica on personal digital devices and make child erotica available to other internet users through various file-sharing interfaces.

SA Seder will further testify regarding file transfer protocols and peer to peer file sharing. He will explain where peer to peer client software may be obtained, how it works, and how it is used. He will explain the use of file sharing and peer to peer client software by users and traffickers of child pornography. He will testify regarding how child exploitation investigations are conducted when file transfer protocols and peer to peer client software are in use.

Specifically, he will further testify that BitTorrent is one of many P2P networks. He will explain how a user becomes part of a BitTorrent network, how the user must first obtain BitTorrent software and install it on a device. He will further testify when BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users. SA Seder further will explain how users of a BitTorrent network uses a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. He will explain that a

torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Further he will testify how torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. SA Seder will testify that torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file. In addition, SA Seder will testify how files are downloaded from other users on the BitTorrent network, how a user typically obtains a torrent file, how the BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts or the actual file(s) being sought and how the download of the content is referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software. SA Seder will testify to his investigation conducted using these methods and will render an opinion consistently with his reports and other information that was provided in discovery, including that the Defendant operated the file transfer protocols and peer to peer client software at issue and that the activity on his devices was consistent with the BitTorrent downloads of child pornography that he conducted from the Defendant's devices.

He will opine that the Defendant's devices were not manufactured in Wyoming and that they were manufactured as alleged in the indictment and as shown on any trade inscriptions.

SA Seder' qualifications are further detailed in his curriculum vitae, attached hereto as *Exhibit 1.*

/s/ Gary Seder
SA GARY SEDER
Wyoming Division of Criminal Investigation

INVESTIGATOR DANIEL BROWN, WYOMING DIVISION OF CRIMINAL INVESTIGATION

Qualifications: Daniel Brown is a Wyoming DCI Digital Forensics Investigator stationed in Cheyenne, Wyoming. As part of Investigator Brown's duties with DCI, he conducts forensic analysis of computer evidence obtained during various investigations and operations.

Investigator Brown began working with DCI as an intern in January 2021 before transitioning to full-time employment in his current capacities during August 2022. He has accumulated over 1,000 hours of experience processing and analyzing digital forensic evidence. Investigator Brown has multiple certifications associated with digital forensics, including certifications in Griffeye DI Pro, osTriage, SQLitePrimer, and advanced digital forensic analysis in Microsoft Windows. He also possesses experience utilizing various Cellebrite tools, useful for extracting and viewing information contained on cellular devices.

Prior to joining DCI, Investigator Brown became a Certified PC Technician through Gillette Community College in Gillette, Wyoming, and completed the Law Enforcement Administrative Program through Fox Valley Technical College in Cheyenne, Wyoming. Investigator Brown has a bachelor's degree in Computer Forensics and Digital Investigation through Champlain College in Burlington, Vermont.

Investigator Brown has authored no publications within the past ten years and has not testified as an expert at trial or by deposition within the past four years. Fed. R. Crim. P. 16(a)(1)(G)(iii).

Summary of Testimony: Investigator Brown would testify about his role in this case's investigation and his opinions reached based on that investigation. Specifically, he would testify as to his investigation, preservation, and retrieval of digital information from the digital devices

seized from the Defendant. Investigator Brown would testify regarding the procedures used to preserve and analyze data contained in the Defendant's digital devices with an emphasis upon the forensic download and extraction of that data, particularly via write-blockers and software such as X-Ways, Griffeye DI Pro, Registry Explorer, Tableau TX-1 hardware write-blocker and Axiom. Further, Investigator Brown would discuss data preservation procedures, his analytical procedures, and how he reached conclusions regarding the content associated with the specific offenses charged in this case. Investigator Brown would testify as to what files were found on which of the Defendant's devices and how they were stored on said devices. Investigator Brown will render an opinion consistent with reports and other information provided in discovery, including that the Defendant operated the devices and accounts at issue, that the Defendant used the devices and accounts in the charged conduct, and that the Defendant's accounts and devices were not hacked.

Investigator Brown would further testify how it is extremely common for child pornography users to have messaging applications, social media, email accounts, and cloud storage. Investigator Brown will explain to the jury how different messaging applications, social media, email accounts, and cloud storage platforms operate, and how individuals upload files, photos and videos on servers, to such online accounts which allows members to access them from any digital devises with an internet or data connection. Investigator Brown will further explain how individuals use messaging applications, social media, email, and cloud storage to share different types of media without physically storing information on their own personal digital/electronic devices and how that information can be downloaded to a device. He will explain that using mobile devices to access messaging applications, social media, email accounts, peer to peer file sharing, and cloud storage uses a combination of the internet and

cellular telephone networks. He will explain that using computers to access messaging applications, social media, email accounts, peer to peer file sharing, and cloud storage uses the internet.

Investigator Brown would explain that it is common for child pornography distributors and possessors to store contraband on personal digital/electronic devices and make illicit content available to other internet users through various file-sharing interfaces. He will explain that it is also common for child pornography distributors and possessors to store child erotica on personal digital/electronic devices and make child erotica available to other internet users through various file-sharing interfaces.

Investigator Brown will further testify regarding file transfer protocols and peer to peer file sharing. He will explain where peer to peer client software may be obtained, how it works, and how it is used. He will explain the use of file sharing and peer to peer client software by users and traffickers of child pornography. He will testify regarding how child exploitation investigations are conducted when file transfer protocols and peer to peer client software are in use.

Specifically, he will further testify that BitTorrent is one of many P2P networks. He will explain how a user becomes part of a BitTorrent network, how the user must first obtain BitTorrent software and install it on a device. He will further testify when BitTorrent software is running and the device is connected to the Internet, the user will be able to download files from other users on the network and share files from their device with other BitTorrent users. Investigator Brown will explain how users of a BitTorrent network uses a BitTorrent program to create a "torrent" file for the file or group of files they wish to share. He will explain that a

torrent file is a small file that contains information about the file(s) and provides a method for a user to download the file(s) referenced in the torrent from other BitTorrent users. Further he will testify how torrent files are typically found as the result of keyword searches on Internet sites that host or link to them. Investigator Brown will testify that torrent files may be referenced by their "infohash", which uniquely identifies the torrent based on the file(s) associated with the torrent file. In addition, Investigator Brown will testify how files are downloaded from other users on the BitTorrent network, how a user typically obtains a torrent file, how the BitTorrent software processes the information in the torrent file and locates devices on the BitTorrent network sharing all or parts or the actual file(s) being sought and how the download of the content is referenced in the torrent is achieved after the requesting computer and the sharing computer(s) directly connect to each other through the Internet using the BitTorrent software. Investigator Brown will testify to his investigation conducted using these methods and will render an opinion consistently with his reports and other information that was provided in discovery, including that the activity on the Defendant's devices was consistent with the BitTorrent downloads of child pornography conducted by SA Seder, Defendant operated the file transfer protocols and peer to peer client software at issue.

He will opine that the Defendant's devices were not manufactured in Wyoming and that they were manufactured as alleged in the indictment and as shown on any trade inscriptions.

Investigator Brown's qualifications are further detailed in his curriculum vitae, attached hereto as *Exhibit 2.*

/s/ Daniel Brown
INVESTIGATOR DANIEL BROWN
Wyoming Division of Criminal Investigation

The United States asserts that this notice and the reports previously provided to the Defendant, as well as the actual files obtained from the Defendant's electronic devices and online accounts, satisfy the requirements of Rule 16(a)(1)(G). If, after viewing this notice and the attachments, the Defendant requests further information or has concerns under Rule 16, the United States requests the Defendant advise as to what further information is necessary to prepare for trial.

Respectfully submitted this 8th day of January, 2024.

NICHOLAS VASSALLO
United States Attorney

By: */s/ Christyne M. Martens*
CHRISTYNE M. MARTENS
Assistant United States Attorney

CERTIFICATE OF SERVICE

I hereby certify that on January 8th, 2024, the foregoing was filed via CM/ECF and thereby served upon counsel for the Defendant.

/s/ Lisa Wait
UNITED STATES ATTORNEY'S OFFICE